PCT/EP2004/012137

Europäisches Patentamt | European Patent Office | Office européen des brevets

27.10.2004

REC'D 19 NOV 2004

WIPO PCT

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03024771.2

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Offic

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03024771.2
Demande no:

Anmeldetag:
Date of filing: 29.10.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Sony Ericsson Mobile Communications AB

221 88 Lund
SUEDE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Binding content to a user

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G06F1/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR LI

Binding content to a user

There is a trend within the field of tele- and computer communication to be able to download content, for instance different types of media content like music, from different content providers. In this regard it is necessary that the content is used according to the conditions set out by the content provider. In order to do this the content is often encrypted and provided with a rights object setting out the terms for the use of the content in question. A user might for instance be allowed to play a piece of music a fixed number of times or within a specified time limit.

One environment in which this can take place is set out for the area of mobile phones by OMA (Open Mobile Alliance), which are setting up a DRM (Digital Rights Management) scheme, OMA DRM, for handling of such rights objects. This scheme sets out a number of supported features, which allows a user to download content and use the content on a device to which the content was downloaded under the conditions set out by the content provider.

Binding content to a user, the SIM constraint

1 Background

Flat rate subscriptions with unlimited content download is a possible business model for OMA DRM. With the current mechanisms there is a possibility for fraud. The fraud scenario is as follows:

1. User A has a flat rate subscription
2. User A removes his SIM and inserts it in user Bs phone.
3. User A downloads content to user Bs phone
4. User B inserts his SIM in his phone.
5. User B can now use the content downloaded by user A

Note that changing SIM is only necessary when SIM authentication is used towards the download service. If username password is used then all user A has to do is share his password with user B.

Another remark is that this is very difficult if not impossible to prevent this if the authentication mechanism for the subscription is susceptible to cloning attacks. In our environment this can only be prevented if the authentication is based on some reasonably secure hardware such as a SIM.

Therefore we will only suggest SIM based prevention mechanisms in this document.

2 Client based enforcement

In a client based solution the natural way is to add a constraint to the REL indicating allowed SIMs. This constraint would then be evaluated and enforced as an integrated part of the DRM framework.

The natural choice is to bind the RO to the IMSI on the SIM. This can be done in two ways:

- The constraint (IMSI) is added to the RO by the rights issuer
- The constraint (IMSI) is added to the RO automatically by the DRM agent in the client.

To further enhance the flexibility of the scheme it shall be possible to bind the RO to a group of SIMs. Here we can utilize the SIM personalization categories:

- Bind to network, MCC and MNC digits of the IMSI
- Bind to network subset, Digit 6-7 of the IMSI
- Bind to service provider, GID 1 and MCC and MNC digits of the IMSI
- Bind to corporate , GID 2and MCC and MNC digits of the IMSI
- Bind to SIM, entire IMSI

If we put this together into REL syntax we get the following:

```
< BindToSIM >
        < Network >
                [AUTOLOCK] | "123456"
        </ Network >
        < Subset >
                [AUTOLOCK] | "78"
        </ Subset >
        < ServiceProvider >
                [AUTOLOCK] | "123456" | "0xFF..."
        </ ServiceProvider >
        < Corporate >
                [AUTOLOCK] | "123456" | "0xFF..."
        </ Corporate >
        < IMSI >
                [AUTOLOCK] | "123456789..."
        </ IMSI >
</ BindToSIM >
```

The syntax for the IMSI and GID1 values can be further enhanced by allowing wildcards (?|*).

AUTOLOCK indicates that the DRM agent will automatically bind the RO to the SIM that is currently inserted using the category defined in the RO. This is done once, i.e. when the RO first arrives in the client.

It is also possible to always automatically bind the RO to the SIM even if this is not indicated by a constraint in the RO. For a proprietary solution where we don't want to modify the REL this would be the preferred approach. Furthermore whether we support the proprietary solution or not shall be a part of the customization offering.

If the RO delivery method is not considered secure enough to hide the IMSI value this can be achieved by inserting a hash of the IMSI instead of the actual value. It should be noted that this prevents the use of wildcards since the hash values must match exactly.

When we introduce this feature as a proprietary extension we must also consider how non compliant phones will react. A well behaving non compliant device will ignore this constraint. In this case our original fraud scenario is till possible as long as device B is non compliant. One solution is that the RI Don't send ROs to non compliant phones. This filtering mechanism could for example be based on the information in UA-prof.

There has been some concern that the AUTOLOCK feature would lead to some difficult error cases. One such case would be that user A has a RO subscription and that user B borrows the phone. The fear is that when the RO it is automatically bound to User B instead of user A. This will not happen since that would imply that user B would start receiving SMS and push sent to A when using As phone with his own SIM.

In fact the problem related to RO subscriptions that can arise will do so even without binding content to a user. Consider the following scenario: User A has a RO subscription and he borrows another phone and inserts his SIM. As long as he has his SIM inserted in the borrowed phone his subscription ROs will be sent to that DRM client. Now he switches back and his subscription ROs are stuck without salvation in the previous phone.

Other solutions are possible but in general they would involve key establishment mechanisms between the RI and compliant handsets. This path is not feasible in the short term since this type of mechanisms is currently being defined for OMA release 2.

3 Server based fraud detection

If SIM based authentication is used it may be possible to introduce network based fraud prevention mechanisms.

One such possibility is to fetch the IMEI from the HLR each time a user requests a new RO. This way the service could detect if a user downloads content to several phones. Apparent fraudsters could than be blocked from using the service.

Sony Ericsson

Binding content to a user, the SIM constraint

Problem

1. User A has a flat rate subscription
2. User A removes his SIM and inserts it in user Bs phone.
3. User A downloads content to user Bs phone
4. User B inserts his SIM in his phone.
5. User B can now use the content downloaded by user A

Sony Ericsson

Solution

Bind the RO to the IMSI on the SIM:

- The constraint (IMSI) is added to the RO by the rights issuer
- The constraint (IMSI) is added to the RO automatically by the client

Bind the RO to the SIM when the RO first arrives in the client:

- AUTOLOCK constraint in the Rights expression language
- Always bind the RO to the SIM. For a proprietary solution this is the preferred approach since it requires no modification of the REL.

Claims

1. A method of providing information about digital rights management features in relation to an electronic communication device comprising the steps of:

-providing a downloadable content,
-providing a right object (RO),
-binding the content to a user such that a constraint is added to the right object (RO).

2. The method according to claim 1, wherein the constraint is added by a rights issuer.

3. The method according to claim 1, wherein the constraint is added automatically in the communication device.

4. The method according to claim 3, wherein the constraint is added by means of a DRM-agent.

5. The method according to claim 3, wherein the right object (RO) is added to a subscriber indentification module (SIM) when the right object (RO) first arrives in the communication device.

6. The method according to claim 1, wherein the right object (RO) is always added to the SIM.

7. Electronic communication device for communication with a content provider and comprising:

-a digital rights management control unit arranged to provide:
binding content to a user, such that a constraint is added to a right object (RO).

8. Electronic communication device according to claim 7, wherein an IMSI is added to the right object (RO).

9. System for managing digital rights management features in relation to an electronic communication device comprising:
an electronic communication device for communication with a content provider and comprising:

-a digital rights management control unit arranged to provide:
binding content to a user, such that a constraint is added to a right object (RO),
-a content provider providing
a downloadable content, and a right object (RO) said system being arranged to provide binding content to a user, such that a constraint is added to a right object (RO).

10. Computer program product for providing information for providing information about digital rights management features in relation to an electronic communication device comprising a computer readable medium having thereon:

computer program code means, to make the electronic communication device execute, when said program is loaded in the electronic communication device:

-providing a downloadable content,
-providing a right object (RO),
-binding the content to a user such that a constraint is added to the right object (RO).